REMARKS

The following remarks are responsive to the Non-Final Office Action of October 24, 2008.

At the time of the Office Action, claims 1- 23 were pending. The status of the claims is as follows:

- Claims **5 and 19** were objected to as lacking antecedent basis for the first and second factors and variables s and c;
- Claims **1–14 and 16** were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter;
- Claims **1–23** were rejected under 35 U.S.C. §112, second paragraph as being indefinite; and
- Claims **1–23** were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 2006/0072743 to **Naslund**, et al.

Applicants have amended claims 1, 10, and 17 in order to more distinctly claim the invention.

OBJECTION TO CLAIMS 5 AND 9

1. Applicants have amended claims 5 and 19, and base claims 1 and 17 to provide the proper antecedent basis for the first factor (s) and the second factor (c).

In the Office Action, on p. 2, the Examiner objected to claims 5 and 19 as lacking antecedent basis for the reference to (s, c). In response, Applicants have amended claims 5 and 19, and base claims 1 and 17 to provide the proper antecedent basis for the first factor (f_1) and the second factor (f_2). Having fully addressed the Examiner's basis for the objection, Applicants respectfully request that this objection be withdrawn from the application.

35 U.S.C. §101 USEFULNESS OF CLAIMS 1–14 AND 16

2. Applicants have amended independent claim 1, and have provided a processor so that the claims are now directed to a machine, which constitutes statutory subject matter.

In the Office Action, on pp. 2–3, the Examiner rejected claims 1–14 and 16 as being directed to non-statutory subject matter, indicating that the language of claim 1 is directed to a method of manipulating numbers, which is an abstract idea. The Examiner indicated that there is no concrete, tangible result defined in claim 1.

Applicants presume the Examiner is referring to the standard established in *State Street Bank* related to the "useful, concrete, and tangible result". However, *In re Bilski* superseded this criteria and put in its place the present "machine or transformation" test.

Applicants have amended claim 1 so that it provides for a processor of the device. This brings it within the statutory category of a machine, and thus, this amendment results in a proper method claim. Furthermore, Applicants language introduced subsequent to the "thereby" clause provide for the utility of the claim by introducing successive physical steps instead of results or successive mathematical relationships.

It is clear to any person of ordinary skill in the corresponding art that selecting and memorizing the first and second factors cannot be performed by the human brain, whatever the skill degree of mental calculation capacity of the latter is, particularly in their binary representation.

Shifting the first factor in accordance to the positions of the bits set to 1 of the second factor cannot be either performed by the human brain. Instead corresponding operations must be performed in an addressable memory only, which further supports the statutory nature under the "machine or transformation" test. The same is true for assembling the successive shifted binary versions of the first factor.

It is clear to any person of ordinary skill in the corresponding art that implementing and carrying out the arithmetic multiplication operation by shifting and assembling *only* would serve to drastically reduce the costs of computing time and/or to allow to reduce substantially the complexity of the arithmetic computing unit which has to complete bit of same rank summation only. See particularly U.S. Patent Publication No. 2008/0137844 at paragraph [0047] in which a number n of shifted binary versions are summed only to a binary number representing the result of the multiplication operation, thus of the arithmetic multiplication operation.

For these reasons, Applicants respectfully assert that the claim language, as amended, is statutory and respectfully requests that the Examiner withdraw the 35 U.S.C. §101 rejection from

the application. If the Examiner understands that these amendments do not appear to satisfy the requirement of usefulness, the Examiner is invited to suggest appropriate language for doing so or to contact the undersigned attorney of record.

35 U.S.C. §112, SECOND PARAGRAPH, INDEFINITENESS OF CLAIMS 1–23

3. Applicants have amended claims 1, 5, 9–11, 13, 17, 19, 21, and 22 to eliminate the language indicated by the examiner as being narrative and indefinite and to address the confusion over the named variables and language associated therewith .

In the Office Action, on pp. 3–4, the Examiner rejected claims 1–23 as being indefinite and failing to conform to U.S. practice. Applicants have amended claims 1, 10, and 17 to eliminate the language indicated by the examiner as being narrative and indefinite. Particularly, the method claims have been amended to begin with a gerund which conforms to U.S. practice. Applicants have further amended device claim 17 to that the means language conforms more closely to that permitted under 35 U.S.C. §112, ¶6.

Furthermore, Applicants have amended the variable definitions provided in order to help avoid confusion. Referring to the published patent application, in paragraphs [0047]–[0048], the following variables are identified: first factor (f_1), second factor (f_2), secret key (s), pseudo-random challenge (c), cryptographic value (y). In one embodiment of the invention, the first factor f_1 is the secret key s, and the second factor f_2 is the pseudo-random challenge c provided by the security application. However, Applicants have delineated between the variables in the claim language for clarification.

Applicants respectfully assert that the claim amendments address the Examiner's basis for the §112 rejection and request that this rejection be removed from the application. As with the preceding section above, if the Examiner understands that these amendments do not appear to satisfy the requirement of definiteness, the Examiner is invited to suggest appropriate language for doing so or to contact the undersigned attorney of record.

35 U.S.C. §102(e) ANTICIPATION OF CLAIMS 1–23 BY NASLUND

4. Applicants have amended independent claims 1and 17 to more distinctly claim the invention; Naslund does not teach or suggest the step of carrying out the multiplication operation step of the present invention as currently claimed.

In the Office Action, on p. 3–4, the Examiner rejected claim 1 as being anticipated by Naslund, and identified how Naslund was being read on each of the elements of the claim. The Examiner stated:

> As per claim 1, Naslund teaches a method for performing a cryptographic operation in a device under the control of a security application, in which a cryptographic value (y) is produced in the device, by a calculation comprising at least one multiplication between two factors including a part at least of a secret key (s)associated with the device (0275),
>
> wherein the first of the two factors of the multiplication has a determined number of bitsL in binary representation, the second of the two factors of the multiplication isconstrained so that it comprises, in binary representation, several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L - 1 bits set to 0,and the multiplication is achieved by assembling binary versions of the first factor, respectively shifted in accordance with the positions of the bits set to 1 of the second factor (0276).

Applicants respectfully disagree with this characterization of the teaching of Naslund. Naslund addresses a method of key exchange (e.g., see Naslund, claims 21 to 26), in which base coefficients are processed in parallel in order to generate a secure key. In the present invention, the successive shifting of the first factor cannot be construed as such parallel processing.

Furthermore, Naslund's disclosure of calculating $yA = g^{xA}$ and $yB = g^{xB}$ from the first and second base coefficients cannot be performed by carrying out a simple arithmetic multiplication operation. Additionally, there is no disclosure of, and in fact it appears unlikely that the exponentiation calculation that is needed by Naslund can be obtained by shifting and assembling factors expressed in their binary form. Instead, corresponding exponentiation calculations are carried out via the finite field cryptography unit (FFCU 2145, Fig. 24A). Naslund, at paragraph [0254] describes the FFCU as "using one or more processing units of a conventional computer or of a hand-held device such as a mobile phone". This is clearly at odds with the aims of the present invention which is to avoid the use of such complex forms of processors.

Also, Naslund deals with operations in a finite field, whereas the present invention deals with multiplication of integers—these the relevant calculations are completely different from one another.

Naslund states, at paragraphs [0275] and [0276] cited by the Examiner:

> **[0275]** The second converser generates a number r (e.g., using a random-number generator or pseudo-random-number generator that can be incorporated, for example, into the key source **2413**) and calculates a pair of quantities (u, v)=(g^r, $f^{-1}(P)*(yA)^r$) using the FFCU **2415** (e.g. a processing unit), wherein P represents a plaintext message of a set of plaintext messages, f is a mapping function that maps at least a portion of a vector space over F to the set of plaintext messages, and * denotes a suitable binary operation on the vector space over F (step **2603**). Additional details relating to the mapping function f, the vector space over F and the operation * will be described below and with reference to **FIG. 27** (which addresses the case where g is an element of F) and **FIG. 28** (which addresses the case where g is a point on an elliptic curve over F).
>
> **[0276]** The number r can be a randomly or pseudorandomly generated integer as these terms are conventionally understood in the art. The number r is not intended to be shared with other conversers, and, in this regard, can be considered a secret number. To calculate the quantity v, multiple groups of first data bits representing at least some of the plural first base coefficients of yA are stored in a first register and processed in parallel. The multiple groups of first data bits can be stored in the first register such that at least one first guard bit is positioned adjacent to the most significant bit of each group of first data bits, each group of first data bits being separated from an adjacent group of first data bits by a corresponding at least one first guard bit. In other words, either the single-guard-bit representation or the multiple-guard-bit representation can be used. An initial value of zero can be assigned to each first guard bit. Where, g is chosen to be an element of F, the exponentiation of yA can be carried according to equation 32 described previously. Where g is chosen to be a point on an elliptic curve over F, the exponentiations associated with $(yA)^r$ and g^{xA} denote r-fold (or xA-fold) elliptic-curve point addition.

Applicants are not certain which portions of this disclosure the Examiner is equating to the first and second factors, and specifically how this disclosure reads on the shifting as required by the claims.

Nonetheless, Applicants understand that the amended claim language serves to clearly delineate over the disclosure of Naslund, and respectfully asks that, in the event this rejection is maintained, that the Examiner clearly identify which specific portions of the disclosure of Naslund read on each of the claimed elements.

Applicants assert that the arguments made with respect to independent claim 1 are also applicable to independent claim 17, and also to the remaining dependent claims by virtue of their dependence.

Given the amendments to the claims and the arguments presented above, Applicants respectfully request that the Examiner withdraw the 35 U.S.C. §102 rejection from the application.

CONCLUSION

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney(s).

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
Mark Bergner, Reg. No. 45,877
Attorneys for Applicant(s)
DRINKER BIDDLE & REATH LLP
191 North Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: February 9, 2009

CH01/ 25298663.1